

## BACKGROUND PAPER TO NEWS RELEASE OF FEBRUARY 22, 2000:

### Manitoba Division of Driver and Vehicle Licencing Follows Ombudsman's Office Recommendations

The Ombudsman's Office has concluded its special investigation into security arrangements in relation to the transfer of personal information, held by Manitoba Highways and Government Services (then Manitoba Highways and Transportation), to the Office of the Chief Electoral Officer of Canada. The personal information was obtained to update the National Register of Electors. It was brought to the attention of our Office that a large volume of personal information that had been provided by the Division of Driver and Vehicle Licencing (DDVL) to Elections Canada had disappeared. The investigation was initiated to determine whether the personal information had been protected in the manner required by s.41 of *The Freedom of Information and Protection of Privacy Act* (FIPPA):

#### **Protection of personal information**

**41** *The head of a public body shall, in accordance with any requirements set out in the regulations, protect personal information by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction.*

This investigation was conducted pursuant to Part 4, Powers and Duties of the Ombudsman, under FIPPA. In accordance with s.49 of FIPPA, the Ombudsman's Office may conduct investigations, provide comments, and make recommendations on access and privacy matters:

#### **General powers and duties**

**49** *In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may*

- (a) conduct investigations and audits and make recommendations to monitor and ensure compliance*
  - (i) with this Act and the regulations,*
- (d) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs of public bodies;*
- (e) comment on the implications for protection of privacy of*
  - (i) using or disclosing personal information for record linkage, or*
  - (ii) using information technology in the collection, storage, use or transfer of personal information;*
- (g) recommend to a public body, after giving the head an opportunity to make representations, that the public body*
  - (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act,*
- (h) make recommendations to the head of a public body or the responsible minister about the administration of this Act;*
- (i) consult with any person with experience or expertise in any matter related to the purposes of this Act;*

The investigation included conducting interviews with DDVL personnel and reviewing materials from DDVL files. Some of the records in the custody or under the control of DDVL that were reviewed originated with Elections Canada. The Ombudsman's Office has kept the disclosure of information from these records to the minimum amount necessary to fulfill its reporting obligations under FIPPA.

## EXCERPTS FROM THE OMBUDSMAN'S REPORT AND RECOMMENDATIONS

Elections Canada has established an electronic National Register of Electors. This computer database contains personal information about millions of Canadian voters, including such information as their names, addresses, and dates of birth. To keep the information current, the database is updated on a quarterly basis. The updated information is provided by provincial and territorial government agencies that collect drivers' licence information or vital statistics.

Elections Canada negotiated a one-year interim agreement with the government of Manitoba in July 1998. The agreement pertained to the disclosure of personal information about all Manitoba drivers over the age of 18 to Elections Canada. The agreement provided for exceptions to disclosure in cases where individuals were listed in the DDVL protected database or had opted out of the provincial voters registry. The DDVL maintains a protected data base that is used, at the person's request, to prohibit the disclosure of personal information from the drivers' licence records to a third party in cases where the personal safety and security of that person may be at risk. Individuals may "opt out" of the provincial voters registry or may choose to have their names obscured from the voters list for reasons of personal security protection.

In September 1998, the first aggregate of electronic data was sent by the DDVL to Elections Canada. The tape containing the data was in a plastic cartridge, measuring 4" x 5" x 1". It included the names, gender, dates of birth, civic addresses, mailing addresses, and drivers' licence numbers of about 675,000 drivers in Manitoba.

In October 1998, the DDVL met with the Ombudsman's Office to discuss the requirements under FIPPA concerning consent and notification under the agreement with Elections Canada. We agreed to provide the Division with a formal *Comment*, pursuant to Part 4 of FIPPA. On February 9, 1999, before the Ombudsman's Office learned of the disappearance of the information, a formal *Comment* was provided to the DDVL. The document conveyed our Office's opinion about the appropriateness of the disclosure under the interim agreement to Elections Canada of personal information in the custody or under the control of the DDVL in the context of the requirements under FIPPA, and about the matter of informed consent.

## THE INVESTIGATION BY THE OMBUDSMAN'S OFFICE

Because the Ombudsman's jurisdiction does not extend beyond Manitoba's borders, the Office was unable to investigate the disappearance of the data at Elections Canada. Nevertheless, we were able to review information provided by Elections Canada to the DDVL and a summary of conclusions from the Privacy Commissioner of Canada.

The investigation indicated that Elections Canada placed its second quarterly request for the update information from Manitoba on January 11, 1999. The information was delivered to Elections Canada on January 14, 1999. The records appear to have disappeared sometime between the date of delivery to the federal agency (Thursday, January 14, 1999) and the date that the tape was reported missing within the agency (Tuesday, January 19, 1999). Elections Canada notified the DDVL that the information had disappeared nine days later (Thursday, January 28, 1999). In our opinion, this did not constitute prompt notification of the security breach.

Upon receiving notice of the loss, the DDVL promptly advised the executive of Manitoba Highways and Government Services, and acted quickly to suspend further transfers of personal information under the agreement. The Division sent a letter notifying Elections Canada of the suspension on February 2, 1999. The DDVL also informed Elections Manitoba, as an interested party, of the loss. The Ombudsman's Office and the federal Privacy Commissioner's Office were not informed of the incident by either agency. There is no legal requirement that the Ombudsman's Office be notified under these circumstances. It is also observed that a group of key decision-makers was not notified of the loss – the drivers whose personal information disappeared.

FIPPA gives people the right to control their own information, subject to a number of exceptions and circumstances. When public bodies collect personal information, they become custodians of that information. As custodians, public bodies are obliged to do more than protect personal information; they must create open and transparent environments that enable the public to make informed decisions about the collection, use and disclosure of their information. When the provision of personal information is mandatory, in return for goods or services such as drivers' licences, there is a greater onus on public bodies to promote transparency and openness. These principles are achieved through consent and notification.

In a *Comment* about consent and notification in February 1999, the Ombudsman's Office advised the DDVL that the disclosures of personal information to Elections Canada were not authorized under FIPPA. Because the disclosures were not authorized, the Ombudsman's Office indicated that the legislation intends that personal information shall not be disclosed without the direct consent of the individuals the information is about, in this case, Manitoba drivers.

Since the *Comment* was provided, our Office has been considering the elements of fair and informed consent in the context of internationally accepted fair information practices. These practices form part of the principles underlying Manitoba's access and privacy legislation. These practices would suggest that consent should be in writing and should address the elements of informed and direct consent as outlined in Recommendation 8 below.

The Ombudsman's Office also advised that, under FIPPA, it is mandatory for the DDVL to provide notice to individual drivers of all the uses and disclosures of their personal information. Section 37(2) of FIPPA sets out:

**Individual must be informed**

**37(2)** A public body that collects personal information directly from the individual the information is about shall inform the individual of

- (a) the purpose for which the information is collected;
- (b) the legal authority for the collection; and
- (c) the title, business address and telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Elections Canada apparently indicated to the DDVL that the risk of harm from the disappearance of the data was relatively remote and that the loss of the personal information did not appear to be the result of criminal activity or negligence. After conducting an internal investigation, the federal agency concluded the information had been "inadvertently placed in the refuse" and "is now in a garbage bag, buried in the landfill site." Elections Canada reasoned that if the records were inadvertently lost, then any recovery of the information would also be accidental. It found the possibility quite remote that someone would find the information in a landfill.

Elections Canada also indicated that the loss of the Manitoba information was the "first data transfer problem ever experienced". In view of the incident, the agency contracted with a consulting firm to conduct a security audit. When the Ombudsman's Office was made aware of the loss and advised of the security audit, we suggested that it might be appropriate to have an audit conducted by an entirely independent organization such as the Privacy Commissioner of Canada.

The federal Privacy Commissioner subsequently conducted an inquiry and provided the Ombudsman's Office with a summary of conclusions on June 29, 1999 that stated:

*Although Elections Canada already had in place a sophisticated security monitoring system (both human and technical) and well-documented data handling and processing procedures, it undertook to implement a number of recommendations made by the auditors to further enhance its protective security and procedural measures. I have had the opportunity to review the final report and found it to be a very credible and thorough review.*

The agencies involved in the investigation of the disappearance of the records indicated that no evidence was found to suggest that the information had been stolen by either an employee or by means of forced entry. The loss of the tape was attributed to human error and it was concluded that the information was inadvertently placed in the garbage and is now in a landfill site. The Privacy Commissioner concluded:

*I am satisfied that Elections Canada has put in place a number of measures to ensure that this does not happen again, and I do not believe that additional recommendations beyond those already identified are required at this time.*



In the course of our investigation and review of the procedures at Elections Canada, it was discovered that the security and data handling procedures at the DDVL appeared to be considerably less rigorous than those at Elections Canada.

## FINDINGS AND OBSERVATIONS

As a result of our investigation, the Ombudsman's Office concluded that Elections Canada was solely responsible for the unauthorized disclosure or destruction of personal information involved in the disappearance of the records. This is based on the acknowledgment from Elections Canada that the information was delivered to its mailroom on January 14, 1999.

We also concluded that the DDVL acted appropriately in suspending the data transfer agreement promptly with Elections Canada. In addition, the Ombudsman's Office was informed that the missing records did not include the personal information of persons who were on the DDVL's protected database for reasons of personal safety and security or whose personal information had been omitted or obscured from the voters list under the provisions of *The Elections Act of Manitoba*.

The federal agencies were able to establish that the information disappeared while in the custody and control of Elections Canada, but were unable to locate the records. The agencies involved in the investigation of the disappearance concluded that the records had been inadvertently lost.

From the information available to our Office, it is our opinion that there is insufficient evidence to support either position: inadvertent loss or theft. This suggests that adopting either position would be based on some measure of conjecture.

Our Office measured the reasonableness of the security arrangements against the potential risk of harm to the public. It was noted that there is virtually no risk if the information were unintentionally disposed of in the refuse and buried under tons of garbage; there is a higher but limited level of risk if the information were accidentally lost and then found; but there is a much higher level of risk if deliberate theft were involved.

The Ombudsman's Office has considered the possibility that someone would want to gain unauthorized or inappropriate access to this personal information. In these times of "one-to-one marketing" and "relationship marketing", it is possible that someone would wish to obtain a searchable database that included the personal information of some 675,000 adults in the province. This type of database would also be invaluable for conducting data matches with other aggregations, or reconstituting "anonymized" information from statistical reference works.

In this context, we concluded there is a substantial risk of harm to the public if their personal information were illegally used or disclosed. Manitoba drivers must provide personal information to the DDVL in order to obtain a licence. The DDVL does not, however, own the information; it is a custodian of the public's personal information. This means the DDVL has to meet a high

standard in protecting that data and in keeping the public informed about the status of that data in the spirit of openness and transparency.

In considering the reasonableness of security arrangements at the DDVL, the Ombudsman's Office did not restrict itself to the circumstances surrounding the incident in January 1999. We also reviewed some of the general security procedures that provide protection to personal information at the DDVL. It appears that the security measures in place at the DDVL are inadequate to protect the personal information that is being collected, used, and disclosed and that they need to be revised. For example, there seems to be no written procedures specific to the handling of personal information, no consistent procedures that are followed in transmitting or transferring data, no identified personnel to track data, and no audit trails or logs of these transactions. Since the security audit of Elections Canada identified areas for improvement, we believed that an audit of the DDVL would prove to be beneficial. We note that if a loss can occur at Elections Canada, with its stringent security provisions, it is not unreasonable to conclude that a comprehensive audit of the DDVL would be appropriate.

It is significant to note that *The Personal Health Information Act* (PHIA) and its Regulation – FIPPA's companion privacy protection statute – contain more explicit security provisions for trustees and information managers of personal health information than does FIPPA for other personal information. Notwithstanding the acknowledged sensitivity of personal health information, the Ombudsman's Office observes that other personal information may also be extremely sensitive, either as a single record, or in volume or bulk when it is especially susceptible to data linking or matching. It might be assumed that this difference between the Acts reflects, in part, a belief that the information policies, standards, and practices of the Provincial Government would be sufficient to meet the requirements to protect personal information from unauthorized access under, arguably, less explicit statutory requirements. This may not be a safe assumption. Consequently, the Ombudsman's Office suggested to the Department of Highways and Government Services that, in responding to the Office's recommendations, it may find it useful to review the more specific requirements of PHIA and their applicability to personal information in its custody or under its control. With respect to the recommendations below, we note that PHIA calls for an audit of security safeguards at least every two years. This requirement commenced with the proclamation of the legislation on December 11, 1997.

If information can vanish from Elections Canada, in spite of its substantive security measures, there is a considerable risk of a similar occurrence within the much lower security environment at the DDVL. The risk is compounded when it is noted that the DDVL has active agreements to share data with many organizations in addition to Elections Canada.

While the DDVL is not responsible for the loss of information by Elections Canada, it remains accountable for ensuring the transparency of its processes including the use and disclosure of the public's personal information. Public bodies hold personal information as a matter of public trust. Determining whether or not to inform the public of the loss of their personal information requires serious consideration. The principles of transparency and accountability suggest that,

unless there are compelling reasons otherwise, Manitobans should be informed about what has happened to their information.

On November 29, 1999, the Department of Highways and Government Services advised the public of the loss of their personal information.

## OMBUDSMAN'S RECOMMENDATIONS

We understand that Elections Canada would like to reinstate the interim agreement and negotiate a longer-term agreement with the DDVL. Recognizing that Manitobans' personal information has gone astray in a federal jurisdiction outside the authority of FIPPA, I make the following recommendations in the public interest of improving the security of Manitobans' personal information in the custody or under the control of the Department of Highways and Government Services:

- ◆ **RECOMMENDATION 1:**

That the Department of Highways and Government Services undertake a comprehensive audit of the security arrangements for the collection, storage, use, disclosure, retention and destruction of personal information (regardless of the physical form or characteristics of the record) under its data sharing agreements including, but without limiting the audit, such matters as personal information management policies, procedures, and practices established under FIPPA and technical safeguards required in the holding and transfer of personal information to other parties. The objective or standard of the audit should be to ensure a seamless fabric of security from the point of collection through storage and use, to point of disclosure.

- ◆ **RECOMMENDATION 2:**

That the Department of Highways and Government Services identify the mandate, scope and proposed timelines of this audit to the Office of the Ombudsman in its response to our report and recommendations.

- ◆ **RECOMMENDATION 3:**

That the Department provide a detailed implementation schedule to the Ombudsman's Office in relation to the correction of any deficiencies identified by the audit with specific reference to the collection, storage, use, disclosure, retention and destruction of personal information under its data sharing agreements.

- ◆ **RECOMMENDATION 4:**

That the DDVL conduct regular and thorough security audits of its security arrangements for the collection, storage, use, disclosure, retention and destruction of personal information and personal health information, regardless of the physical form or characteristics of the record.

♦ **RECOMMENDATION 5:**

That any future data transfer agreements continue to include provisions for regular and thorough security audits of the other parties to or agencies under a personal information data transfer agreement.

♦ **RECOMMENDATION 6:**

That data transfer agreements include requirements for immediate notification of the Department of Highways and Government Services regarding breaches of security.

♦ **RECOMMENDATION 7:**

That data transfer agreements identify reasonable criteria for public notification regarding breaches of security, to reinforce transparency and accountability.

♦ **RECOMMENDATION 8:**

That the Department of Highways and Government Services obtain informed and direct consent from Manitoba drivers prior to any further transfers of personal information to Elections Canada. The consent should be in writing and address the following:

- (a) the specific personal information to be collected, used or disclosed;
- (b) the identity of the person or public body that the personal information may be collected from, used by, or disclosed to;
- (c) all the purposes for the collection, use or disclosure;
- (d) a statement that the recipient will not use or disclose the personal information except for a purpose specified in the consent, a list of all subsequent uses or disclosures that the recipient of the personal information may make, and any restrictions on those subsequent uses or disclosures;
- (e) an acknowledgement that the consenting individual has been made aware of why the personal information is needed and the risks and benefits to the individual of consenting or refusing to consent to the collection, use or disclosure;
- (f) the date the consent is effective, and the date the consent expires;
- (g) a statement that the consent may be revoked or amended at any time

♦ **RECOMMENDATION 9:**

That the Department of Highways and Government Services notify individual drivers of all the uses and disclosures of their personal information, as required under s.37(2) of FIPPA:

***Individual must be informed***

***37(2) A public body that collects personal information directly from the individual the information is about shall inform the individual of***

- (a) the purpose for which the information is collected;***
- (b) the legal authority for the collection; and***
- (c) the title, business address and telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.***



♦ **RECOMMENDATION 10:**

That the interim data transfer agreement with Elections Canada not be reinstated, and a new agreement not be concluded, until these recommendations of the Ombudsman's Office have been implemented.

**MANITOBA HIGHWAYS AND GOVERNMENT SERVICES' RESPONSE**

In the Ombudsman's Report and Recommendations to the Department of Highways and Government Services dated October 27, 1999, a written response was requested within 15 days indicating either:

1. that the head accepts the recommendations and any action the head has taken or proposes to take to implement them, or
2. the reason(s) why the head refuses to take action to implement the recommendations.

Following are the responses from the Department:

♦ **RECOMMENDATION 1 - 4:**

*The department accepts these recommendations. They are being actively pursued in conjunction with the Information Protection Centre of the Office of Information Technology. DDVL had taken steps prior to your report by reviewing and modifying its procedures for increased security in handling personal data being transferred.*

*We will also provide your office with information regarding the audit timelines and implementation schedule of corrective measures once they have been determined.*

♦ **RECOMMENDATION 5:**

*The Department accepts this recommendation, and will continue to include provision in its personal information data transfer agreements for regular and thorough security audits of the other parties, where the parties do not fall under any privacy legislation, and provided such requirements do not conflict with legislation or government policy which applies to the other contracting party.*

♦ **RECOMMENDATION 6:**

*The Department accepts this recommendation. The Department will continue its practice to require the immediate notification in the event of a security breach.*

♦ **RECOMMENDATION 7:**

*We agree that reasonable criteria for public notification regarding breaches of security needs to be developed. Public notification of a security issue involving personal information and the criteria to be applied are not matters to be addressed in the context of a contract. A contract sets out the rights and obligations of the parties to the contract as between each*

other: it would not be an appropriate vehicle for dealing with broader public interest issues. These policy issues need to be addressed and applied on a case by case basis.

♦ **RECOMMENDATION 8:**

*The Department supports and will follow the principle of transparency of information for the public, including active and informed consent of any future data transfers to Elections Canada. Information (brochures) to address items (a), (b), and (c) of this Recommendation would be circulated to inform the public.*

*The statement outlined in item (d) is not operationally feasible. We would envisage a statement that follows the Revenue Canada approach which outlines the information to be provided, the fact that it will be used for electoral purposes and other uses pursuant to FIPPA.*

*The risks and benefits to the person's consent as outlined in item (e) are not relevant, as a licence would not be refused on the basis of a person refusing to consent.*

*The effective consent date as referenced in item (f) would be addressed through the licence renewal cycle.*

*The revocation or amendment of the consent at any time, as per item (g), would prove to be operationally unworkable. Elections Canada could not systematically reverse personal information provided by one of its data sources.*

♦ **RECOMMENDATION 9:**

*The Department accepts this recommendation. Once the policy decisions are reached by the Government on information disclosure requests by third party users, the Department will be in a position to notify drivers of the information uses and disclosures.*

♦ **RECOMMENDATION 10:**

*If the Department resumes the disclosure of personal information to Elections Canada, a new agreement would not be considered until the Department has met its commitments to your Recommendations.*

## **OMBUDSMAN'S COMMENTS**

♦ **RECOMMENDATION 7:**

We note that the Minister of Manitoba Highways and Government Services issued a news release on November 29, 1999, informing the public of the loss of the tape containing personal information of some 675,000 Manitobans.

In putting forward this recommendation, the intent was to ensure that the Department does have a written policy regarding public notification of security breaches which would provide criteria against which a decision whether or not to notify the public could be gauged.

It may be that a contract is not an appropriate vehicle "...for dealing with broader public interest issues." It is, nevertheless, our opinion that parties with which the Department proposes to contract the use or disclosure of information about an identifiable individual should be aware that public notification of security breaches involving such information is governed by an articulated policy of public notification.

◆ **RECOMMENDATION 8:**

The Ombudsman's Office believes that the Department has substantively accepted Recommendation 8 by supporting and following items (a), (b), and (c) including active and informed consent for any future data transfers to Elections Canada. The implementation of a public information campaign intended to ensure that affected individuals would be able to make an informed choice to give or withhold consent could probably effectively address items (d), (e), (f), and (g). This could include such measures as the distribution of brochures and other information to members of the public affected by the Department's collection, use and disclosure of their personal information. The Ombudsman's Office has no information on which to assess the operational feasibility or unworkability issues brought forward by the Department in its specific responses to items (d) and (g). We will seek additional information from the Department on these matters. The Ombudsman's Office agrees that, in practice, the effective consent and expiry of consent referenced in item (f) would be addressed through the licence renewal cycle. This information should be known to applicants for licences.

A further comment is warranted with respect to items (d) and (e). In offering the elements of consent which should be addressed by a public body or a trustee of recorded information about an identifiable individual, the Ombudsman's Office is not suggesting that there is a single consent form, activity or process by which informed consent may be obtained in the collection, use or disclosure of personal information. It is the duty of public bodies or trustees to ensure that consent is obtained where collection, use or disclosure is not otherwise authorized by legislation. We have put forward generic elements that could, in our opinion, be addressed in a flexible, reasonable, and effective manner so long as the process follows the law and the result is informed consent where it is required. It is the duty of the Ombudsman's Office to provide oversight in this matter. Without prescribing the approach that the Department should take in this case, we are not aware of specific reasons why a public information campaign might not reasonably address (d) and (e). To assist the Department in considering this, we have rearticulated these elements as follows:

(a) a statement from the public body:

- affirming that a third-party recipient will not use or disclose the personal information provided by the public body, except for a purpose specified in the consent, and
- specifying the subsequent disclosures, if any, that the public body permits the third-party recipient to make;

(b) an acknowledgement that the consenting individual has been made aware of:

- why the personal information is needed, and

- the risks and benefits to the individual of consenting or refusing to consent to the collection, use or disclosure;

Addressing each of the elements of consent can contribute to ensuring that the public is providing informed consent and the minimum amount of personal information necessary. The manner in which each element is applied to a particular set of circumstances may be discussed further between our respective offices. For Manitoba Highways and Government Services, it may be that information can be provided in the context of a public communications strategy that has been based on consideration of a range of options such as inserts in licence renewal notices, brochures, posted notices or posters, news releases, and consent forms.

I am confident that these issues can be resolved by working with the Department to develop plans for ensuring informed consent.

♦ **RECOMMENDATION 9:**

The Department accepts the recommendation to provide the statutory notice to drivers, but states that it is not yet in a position to inform them of its uses and disclosures of their personal information. This suggests to us that the Department is awaiting policy decisions on other data-sharing agreements with other third parties. Notwithstanding this, the Department should comply with the notice provisions of FIPPA as soon as possible, in our opinion, since the statutory requirement has been in force since May 1998.

As mentioned previously, notification of the public could encompass a range of options, so long as they comply with the law.

## **FOLLOW-UP TO THE INVESTIGATION**

The Ombudsman's Office is satisfied that Manitoba Highways and Government Services has substantively accepted most of the recommendations in our October 27, 1999 Report. We will monitor the Department's progress and substantive actions in implementing the recommendations, in accordance with the provisions of s.66(6) of FIPPA:

***Compliance with recommendations***

**66(6)** *When the head of a public body accepts the recommendations in a report, the head shall comply with the recommendations*

*(a) within 15 days of acceptance, if the complaint is about access under subsection 59(1), (2) or (4); and*

*(b) within 45 days in any other case;*

*or within such additional period as the Ombudsman considers reasonable.*

A reasonable period for complying with the recommendations will be determined in discussion with the Department. The Ombudsman concluded that any outstanding matters may be resolved by consultation between the Department and the Ombudsman's Office.

**MEDIA CONTACT:** Barry Tuckett or Peter Bower (204) 982-9130 or 1-800-665-0531 (in Manitoba)



# Ombudsman Manitoba

## NEWS RELEASE

750 - 500 Portage Avenue  
Winnipeg, Manitoba R3C 3X1  
Telephone: (204) 982-8130  
Toll Free in Manitoba:  
1-800-665-0531  
Fax: (204) 942-7803  
E-mail: [ombudsman@ombudsman.mb.ca](mailto:ombudsman@ombudsman.mb.ca)  
500 av. Portage, Pièce 750  
Winnipeg (MB) R3C 3X1  
Téléphone : (204) 982-8130  
Sans frais au Manitoba :  
1 800 665-0531  
Télécopieur : (204) 942-7803  
Courriel : [ombudsman@ombudsman.mb.ca](mailto:ombudsman@ombudsman.mb.ca)

For Release February 22, 2000

### Manitoba Division of Driver and Vehicle Licensing Follows Ombudsman's Office Recommendations

**Winnipeg** – The Manitoba Ombudsman's Office has completed an investigation into security arrangements in relation to the transfer of personal information, held by the Division of Driver and Vehicle Licensing (DDVL), to Elections Canada. The Office initiated the investigation in March 1999 to determine whether the personal information had been protected in the manner required by s.41 of *The Freedom of Information and Protection of Privacy Act* (FIPPA). DDVL is a division of the Department of Highways and Government Services.

Barry Tuckett, the Manitoba Ombudsman, found that the disappearance of the computer tape was solely the responsibility of Elections Canada. He also found that personal information collected and disclosed by DDVL has not been protected in the manner required under the legislation.

The investigation was launched on the Ombudsman's own initiative after the Office received information that a large amount of personal information had vanished. The investigation was unable to determine whether the information had been inadvertently lost or deliberately stolen.

The Ombudsman made ten recommendations in his report dated October 27, 1999. Manitoba Highways and Government Services substantively accepted the recommendations in its response of December 6 1999. The Department agreed to:

- conduct a comprehensive audit of its security arrangements for personal information;
- develop reasonable criteria for public notification regarding breaches of security;
- notify Manitoba drivers of the uses and disclosures of their personal information; and
- follow the principle of transparency by providing information to the public, including the seeking of active and informed consent for the disclosure of personal information in any future transfers of such information to Elections Canada.

The Ombudsman observed that there is a positive aspect to the incident in that the publicity generated will help alert other public bodies under FIPPA to the importance of reviewing their security arrangements for personal information.

Perhaps more importantly, the incident serves as a reminder to government departments and agencies that the legislation gives people the right to control their own information, subject to a limited number of exceptions and circumstances.

"When government departments and agencies seek to collect, use or disclose personal information, they should create open and transparent information environments that enable the public to make informed decisions," said the Ombudsman. "When public notification and informed consent become standard operating practices, public confidence in government administration will be enhanced."

The Ombudsman's Office will follow up with Manitoba Highways and Government Services on the implementation of the recommendations to review the Department's progress.

**MEDIA CONTACT:** Barry Tuckett or Peter Bower (204) 982-9130 or 1-800-665-0531 (in Manitoba)

**NOTE:** A **Background Paper** is available from the Ombudsman's Office by contacting the Office by telephone at (204) 982-9130 or 1-800-665-0531 (in Manitoba), or by FAX at (204) 942-7803